IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of: Travis J. Parry	)	Confirmation No: 8466
Serial No.: 10/091,740	)	Group Art Unit: 2132
Filed: March 6, 2002	)	Examiner: Homayounmehr, F.
For: TRANSMITTING DATA ACROSS FIREWALLS	)	Atty. Docket No.: 10013768-1

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop: Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This Appeal Brief under 37 C.F.R. § 41.37 is submitted in support of the Notice of Appeal filed March 23, 2007, responding to the final Office Action mailed January 18, 2007.

It is not believed that extensions of time or fees are required to consider this Appeal Brief. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. §1.136(a), and any fees required therefor are hereby authorized to be charged to Deposit Account No. 08-2025.

I. Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

II. Related Appeals and Interferences

There are no known related appeals or interferences that will affect or be affected by a decision in this Appeal.

III. Status of Claims

Claims 1, 2, 4-14, 17-30, 33-35, 37, and 39-41 stand finally rejected. No claims have been allowed. Claims 3, 15-16, 31-32, 36, and 38 have been canceled. The final rejections of claims 1, 2, 4-14, 17-30, 33-35, 37, and 39-41 are appealed.

IV. Status of Amendments

This application was originally filed on March 6, 2002, with forty-one (41) claims. In a Response filed December 2, 2005, Applicant amended claims 1, 4-6, 9, 13-14, 18-20, 25-27, 29, 33-35, 37, and 39-41 and canceled claims 3, 15-16, 31-32, 36, and 38. In a Response filed March 10, 2006, Applicant presented remarks without any claim amendments. In a Response

filed May 11, 2006, Applicant amended claims 1, 12, 14, 24, 29, and 35. In a Response filed October 24, 2006, Applicant presented remarks without any claim amendments. The claims in the attached Claims Appendix reflect the present state of Applicant's claims.

V. Summary of Claimed Subject Matter

The claimed inventions are summarized below with reference numerals and references to the written description ("specification") and drawings. The subject matter described in the following appears in the original disclosure at least where indicated, and may further appear in other places within the original disclosure.

Embodiments according to independent claim 1 describe a method of transmitting data across a firewall (Figure 1, 20). The method comprises receiving (Figure 4, lines 7-8) a request to transmit data to a destination at a remote network (Figure 1, 40) and searching (Figure 4, 305) for a firewall (Figure 1, 20) associated with the destination at the remote network (Figure 1, 40). The firewall (Figure 1, 20) is configured to prohibit communication to the destination via a primary communication protocol and allow communication to the destination via a secondary communication protocol. The method further comprises automatically configuring (Figure 4, 320) the data for communication with the secondary communication protocol if the firewall is detected. Such a method further comprises transmitting (Figure 4, 330) the data to the destination by utilizing the secondary communication protocol, wherein the request to transmit the data to the destination comprises a primary address of the destination related to the primary communication

protocol and a secondary address of the destination related to the secondary communication protocol. Applicant's specification, pages 8-11, lines 13-7 and pages 17-18, lines 6-17.

Embodiments according to independent claim 14 describe a system for rerouting the transmission of data to avoid a firewall (Figure 1, 20). The system comprises a transmission device (Figure 1, 100) configured to search for a firewall (Figure 1, 20) protecting a destination at a remote network (Figure 1, 40). The firewall (Figure 1, 20) at the remote network (Figure 1, 40) is configured to prohibit communication to the destination via a primary communication protocol and allow communication to the destination via a secondary communication protocol. The transmission device (Figure 1, 100) is further configured to, upon detection of the firewall (Figure 1, 20), automatically configure the data for communication over the secondary communication protocol and transmit the data by utilizing the secondary communication protocol. The transmission device (Figure 1, 100) is further configured to receive a request to transmit the data to the destination and the request comprises at least the following: a primary address and a secondary address of the destination. The primary address is related to the primary communication protocol and the secondary address is related to the secondary communication protocol. The transmission device (Figure 1, 100) is further configured to, upon not detecting the firewall (Figure 1, 20), transmit the data to the destination by utilizing the primary communication protocol. Applicant's specification, pages 8-11, lines 13-7 and pages 17-18, lines 6-17.

Embodiments according to independent claim 29 describe a transmission device (Figure 1, 100) configured to transmit data to a

destination. The transmission device (Figure 1, 100) comprises means for transmitting the data (Pages 14-15, lines 7-6) to the destination at a remote network (Figure 1, 40) by utilizing a secondary communication protocol and means for searching (Page 15, lines 7-21) for a firewall (Figure 1, 20) at the remote network (Figure 1, 40). The firewall (Figure 1, 20) is configured to prohibit communication to the destination by a primary communication protocol and allow communication to the destination via the secondary communication protocol. Such a device further comprises means for automatically configuring the data for communication (Page 15, lines 7-21) for the secondary communication protocol upon detecting the firewall (Figure 1, 20) and means for receiving a request to transmit the data (Pages 14-15, lines 7-6) to the destination, wherein the request comprises at least the following: a primary address and a secondary address of the destination. The primary address is related to the primary communication protocol, and the secondary address is related to the secondary communication protocol. Applicant's specification, pages 8-11, lines 13-7 and pages 17-18, lines 6-17.

Embodiments according to independent claim 35 describe a data transmission program stored on a computer-readable medium. The transmission program (Figure 3, 214) comprises logic configured to facilitate the transmission of data (Pages 14-15, lines 7-6) to a remote network (Figure 1, 40) by utilizing a secondary communication protocol and logic configured to search (Page 15, lines 7-21) for a firewall (Figure 1, 20) at the remote network (Figure 1, 40), wherein the firewall (Figure 1, 20) is configured to prohibit communication to a recipient device at the remote network (Figure 1, 40) via a primary communication protocol and allow communication via the secondary

communication protocol. The program further comprises logic configured to automatically configure communication (Page 15, lines 7-21) for the secondary communication protocol upon detecting the firewall (Figure 1, 20) and logic configured to receive a request to transmit the data (Pages 14-15, lines 7-6) to the recipient device (Figure 1, 60). The request comprises of at least the following: a primary address and a secondary address of the recipient device (Figure 1, 60). The primary address is related to the primary communication protocol, and the secondary address is related to the secondary communication protocol. Applicant's specification, pages 8-11, lines 13-7 and pages 15-18, lines 24-17.

VI. Grounds of Rejection to be Reviewed on Appeal

The following grounds of rejections are to be reviewed on appeal:

Claims 1-2, 4-14, 17-30, 33-35, 37, and 39-41 have been rejected under 35 U.S.C. §102(e) as being anticipated by *Schwartz* (U.S. Patent Application Publication 2002/0199114 A1).

VII. Arguments

Claims 1-2, 4-14, 17-30, 33-35, 37, and 39-41 have been rejected under 35 U.S.C. §102(e) as allegedly being anticipated by *Schwartz* (U.S. Patent Application Publication 2002/0199114 A1).

The Appellant respectfully submits that Applicant's claims 1-2, 4-14, 17-30, 33-35, 37, and 39-41 are patentable under 35 U.S.C. §102. The Appellant respectfully requests that the Board of Patent Appeals overturn the final rejection of those claims at least for the reasons discussed below.

A. The *Schwartz* Disclosure

In general, *Schwartz* teaches embodiments where a transmission device is protected by a firewall and the transmission device attempts to locate an address of the firewall (that is protecting the transmission device) that will allow a connection to be established with the firewall 20 for outside communications.

Accordingly, *Schwartz* discusses how non-traditional devices generally do not have interfaces for configuring the devices for communications with a local firewall. *See* para. 0024. *Schwartz* also discusses how it is necessary for information to be "transferred from the non-traditional devices across from the LAN 311 through the firewall 310 [which services the non-traditional devices] to a destination." *See* Figure 3 and para. 0025. *Schwartz* further discusses how devices often use DHCP to obtain a local IP address for communicating, but that the device may also be configured manually to communicate with the local firewall. Otherwise, an approach of trying different addresses may be used. *See* para. 0026. *Schwartz* also discusses that a connection with a local firewall must be established before communications with entities on the other side of the firewall are possible. *See* para. 0027. *Schwartz* further discusses that a device may sniff packets on a local network to attempt to determine an address and port of a firewall on the local network that allows external communications beyond the firewall. *See* para. 0034.

B. Applicant's Claim 1

As provided in independent claim 1, Applicant claims:

> A method of transmitting data across a firewall, the method comprising:
> ***receiving a request to transmit data to a destination at a remote network;***

> ***searching for a firewall associated with the destination at the remote network***, the firewall being configured to prohibit communication to the destination via a primary communication protocol and allow communication to the destination via a secondary communication protocol;
>
> ***if the firewall is detected, automatically configuring the data for communication with the secondary communication protocol;*** and
>
> transmitting the data to the destination by utilizing the secondary communication protocol, ***wherein the request to transmit the data to the destination comprises a primary address of the destination related to the primary communication protocol and a secondary address of the destination related to the secondary communication protocol***.

(Emphasis added).

Applicant respectfully submits that independent claim 1 is allowable for at least the reason that *Schwartz* does not disclose, teach, or suggest at least "receiving a request to transmit data to a destination at a remote network," "searching for a firewall associated with the destination at the remote network," "if the firewall is detected, automatically configuring the data for communication with the secondary communication protocol," and "wherein the request to transmit the data to the destination comprises a primary address of the destination related to the primary communication protocol and a secondary address of the destination related to the secondary communication protocol," as recited and emphasized above.

Rather, *Schwartz* discloses at most a system for configuring a device to communicate through a firewall on a local network, where the device is also located on the local network. *See* paras. 0024-0025. *See* Figure 3 (*e.g.*, devices 312, 314, and firewall 310). *Schwartz* fails to teach or suggest searching for a firewall associated with a destination at a remote network.

Schwartz also states that "if an address and/or port does not yield a successful connection, then the next time the device will select the most likely address and port 506, it may not include the unsuccessful port." *See* para. 0032. "It is to be understood that select most likely address and port 506 is based upon a database of addresses and ports and that this database changes." *See* para. 0032. Therefore, *Schwartz* fails to teach or suggest that a request to transmit data includes a primary address of the destination that is used if a firewall is not detected and a secondary address of the destination that is used if a firewall is detected, as described in the claim. Rather, *Schwartz* uses whatever port the non-traditional device discerns is most likely to establish a connection with the local firewall. As such, *Schwartz* fails to teach or suggest that a request to transmit data includes a primary address and a secondary address of a firewall associated with a destination. As previously indicated, *Schwartz* teaches that a local device is configured to operate with a local firewall by attempting different addresses for the local firewall. Nowhere does it teach or suggest attempting to communicate with a firewall associated with a destination at a remote network in a manner described by the claim.

For at least these reasons, *Schwartz* fails to anticipate claim 1. In the Office Action of July 24, 2006, it states that "the client shown in Fig. 3 may have to pass the firewall associated with the appliances in the remote network to control them." Page 3. However, nowhere in *Schwartz* does it state that the clients 308-1...308-N shown in Fig. 3 perform the method for firewall traversal disclosed in the reference. Rather, the non-traditional devices 314-1...314-Q are disclosed to employ the method for firewall traversal described

in the reference which states "This information must be transferred from the non-traditional device across the LAN 311 through the firewall 310 to a destination." Para. 0025. Another example is provided in *Schwartz* of a home entertainments system 314-5 that must traverse the local firewall 310 to access the manufacturer's site. As such, *Schwartz* does not teach "searching for a firewall associated with the destination at the remote network . . . wherein the request to transmit the data to the destination comprises a primary address of the destination related to the primary communication protocol and a secondary address of the destination related to the secondary communication protocol," as recited in claim 1.

Moreover, the Office Action of July 24, 2006 states that "It is true that Scharwtz won't try the primary address again if it fails, but it clearly tries it the first time, which was before the connection failed. Therefore, the address of the primary and secondary protocols must be received by the device that initiates the connection." Page 4. Applicant respectfully disagrees, since *Schwartz* teaches that an address may be obtained by sniffing network traffic and therefore does not have to be "received by the device that initiates the connection." Further, *Schwartz* does not teach or suggest that a request to transmit data comprises both the primary address and secondary address of the destination, as described in claim 1.

In the final office action of January 18, 2007, the Examiner asserts that *Schwartz* discloses the searching of a firewall associated with a destination at a remote network and points to paragraph 0025 of the *Schwartz* reference as support. The Examiner construes the non-traditional devices 314-N of Figure 3 that are behind firewall 310 to be at a remote network, from the perspective

of a client 308-N. *See* pages 2-3. However, *Schwartz* does not describe that a client 308-N attempts to build a database of addresses and ports for a remote firewall 311 by sniffing network traffic. Rather, *Schwartz* teaches that the non-traditional devices 314-N attempt to build a database of addresses and ports for the local firewall 311 by sniffing local network traffic. *See* paras. 0033-0034. This is because *Schwartz* is focused on a local client device attempting to find a port of a local firewall that allows the client device to communicate with remote devices. *See* para. 0034.

In the final office action of January 18, 2007, the Examiner also states that "Schwartz does try a primary address and if it fails a connection it tries the second address. . . . Therefore, the address of the primary and secondary protocols must be received by the device that initiates the connection." Pages 3-4. In response, Applicant observes that the Examiner has failed to show that a request to transmit data to a destination comprises both a primary address of the destination and a secondary address of the destination.

For at least these reasons, *Schwartz* fails to anticipate claim 1, and the rejection of claim 1 should be withdrawn for at least the aforementioned reasons.

C. Applicant's Claims 2 and 4-13

Because independent claim 1 is allowable over the cited art of record, dependent claims 2 and 4-13 (which depend from independent claim 1) are allowable as a matter of law for at least the reason that the dependent claims 2 and 4-13 contain all the features of independent claim 1. For at least this reason, the rejection of claims 2 and 4-13 should be withdrawn.

Additionally and notwithstanding the foregoing reasons for allowability of claims 2 and 4-13, these claims recite further features and/or combinations of features (as is apparent by examination of the claims themselves) that are patentably distinct from the cited art of record. Hence, there are other reasons why these dependent claims are allowable.

Accordingly, the rejections to these claims should be withdrawn.

D. Applicant's Claim 14

As provided in independent claim 14, Applicant claims:

> A system for rerouting the transmission of data to avoid a firewall, the system comprising: a transmission device configured to ***search for a firewall protecting a destination at a remote network***, the firewall at the remote network being configured to prohibit communication to the destination via a primary communication protocol and allow communication to the destination via a secondary communication protocol, the transmission device is further configured to, ***upon detection of the firewall, automatically configure the data for communication over the secondary communication protocol and transmit the data by utilizing the secondary communication protocol, wherein the transmission device is further configured to receive a request to transmit the data to the destination and the request comprises at least the following: a primary address and a secondary address of the destination, the primary address being related to the primary communication protocol and the secondary address being related to the secondary communication protocol and wherein the transmission device is further configured to, upon not detecting the firewall, transmit the***

data to the destination by utilizing the primary communication protocol.

(Emphasis added).

Applicant respectfully submits that independent claim 14 is allowable for at least the reason that *Schwartz* does not disclose, teach, or suggest at least a transmission device configured to "search for a firewall protecting a destination at a remote network," "upon detection of the firewall, automatically configure the data for communication over the secondary communication protocol and transmit the data by utilizing the secondary communication protocol," and "wherein the transmission device is further configured to receive a request to transmit the data to the destination and the request comprises at least the following: a primary address and a secondary address of the destination, the primary address being related to the primary communication protocol and the secondary address being related to the secondary communication protocol and wherein the transmission device is further configured to, upon not detecting the firewall, transmit the data to the destination by utilizing the primary communication protocol," as recited and emphasized above.

Rather, *Schwartz* discloses at most a system for configuring a device to communicate through a firewall on a local network, where the device is also located on the local network. *See* paras. 0024-0025 and Figure 3 (*e.g.*, devices 312, 314, and firewall 310). *Schwartz* fails to teach or suggest searching for a firewall protecting a destination at a remote network.

Schwartz also states that "if an address and/or port does not yield a successful connection, then the next time the device will select the most likely address and port 506, it may not include the unsuccessful port." *See* para.

0032. "It is to be understood that select most likely address and port 506 is based upon a database of addresses and ports and that this database changes." *See* para. 0032. Therefore, *Schwartz* fails to teach or suggest that a request to transmit data includes a primary address of the destination that is used if a firewall is not detected and a secondary address of the destination that is used if a firewall is detected, as described in the claim. Rather, *Schwartz* uses whatever port the non-traditional device discerns is most likely to establish a connection with the local firewall. As such, *Schwartz* fails to teach or suggest that a request to transmit data includes a primary address and a secondary address of a firewall associated with a destination. As previously indicated, *Schwartz* teaches that a local device is configured to operate with a local firewall by attempting different addresses for the local firewall. Accordingly, nowhere does it teach or suggest attempting to communicate with a firewall associated with a destination at a remote network in a manner described by the claim.

For at least these reasons, *Schwartz* fails to anticipate claim 14. In the Office Action of July 24, 2006, it states that "the client shown in Fig. 3 may have to pass the firewall associated with the appliances in the remote network to control them." Page 3. However, nowhere in *Schwartz* does it state that the clients 308-1...308-N shown in Fig. 3 perform the method for firewall traversal disclosed in the reference. Rather, the non-traditional devices 314-1...314-Q are disclosed to employ the method for firewall traversal described in the reference which states "This information must be transferred from the non-traditional device across the LAN 311 through the firewall 310 to a destination." Para. 0025. Another example is provided in *Schwartz* of a home

entertainments system 314-5 that must traverse the local firewall 310 to access the manufacturer's site. As such, *Schwartz* does not teach to "search for a firewall protecting a destination at a remote network . . . wherein the transmission device is further configured to receive a request to transmit the data to the destination and the request comprises at least the following: a primary address and a secondary address of the destination, the primary address being related to the primary communication protocol and the secondary address being related to the secondary communication protocol and wherein the transmission device is further configured to, upon not detecting the firewall, transmit the data to the destination by utilizing the primary communication protocol," as recited in claim 14.

Moreover, the Office Action of July 24, 2006 states that "It is true that Scharwtz won't try the primary address again if it fails, but it clearly tries it the first time, which was before the connection failed. Therefore, the address of the primary and secondary protocols must be received by the device that initiates the connection." Page 4. Applicants respectfully disagree, since *Schwartz* teaches that an address may be obtained by sniffing network traffic and therefore does not have to be "received by the device that initiates the connection." Further, *Schwartz* does not teach or suggest that a request to transmit data comprises both the primary address and secondary address of the destination, as described in claim 14.

For at least these reasons, *Schwartz* fails to anticipate claim 14, and the rejection of claim 14 should be withdrawn.

E. Applicant's Claims 17-28

Because independent claim 14 is allowable over the cited art of record, dependent claims 17-28 (which depend from independent claim 14) are allowable as a matter of law for at least the reason that the dependent claims 17-28 contain all the features of independent claim 14. For at least this reason, the rejection of claims 17-28 should be withdrawn.

Additionally and notwithstanding the foregoing reasons for allowability of claims 17-28, these claims recite further features and/or combinations of features (as is apparent by examination of the claims themselves) that are patentably distinct from the cited art of record. Hence, there are other reasons why these dependent claims are allowable.

Accordingly, the rejections to these claims should be withdrawn.

F. Applicant's Claim 29

As provided in independent claim 29, Applicant claims:

> A transmission device configured to transmit data to a destination, the transmission device comprising:
>
> means for transmitting the data to the destination at a remote network by utilizing a secondary communication protocol;
>
> ***means for searching for a firewall at the remote network, the firewall being configured to prohibit communication to the destination by a primary communication protocol and allow communication to the destination via the secondary communication protocol;***
>
> ***means for automatically configuring the data for communication for the secondary communication protocol upon detecting the firewall; and***
>
> ***means for receiving a request to transmit the data to the destination, wherein the request comprises at least the following:***
>
> ***a primary address and a secondary address of the destination, the primary address being related to the primary communication protocol and the secondary***

address being related to the secondary communication protocol.

(Emphasis added).

Applicant respectfully submits that independent claim 29 is allowable for at least the reason that *Schwartz* does not disclose, teach, or suggest at least "means for searching for a firewall at the remote network, the firewall being configured to prohibit communication to the destination by a primary communication protocol and allow communication to the destination via the secondary communication protocol," "means for automatically configuring the data for communication for the secondary communication protocol upon detecting the firewall," and "means for receiving a request to transmit the data to the destination, wherein the request comprises at least the following: a primary address and a secondary address of the destination, the primary address being related to the primary communication protocol and the secondary address being related to the secondary communication protocol," as recited and emphasized above.

Rather, *Schwartz* discloses at most a system for configuring a device to communicate through a firewall on a local network, where the device is also located on the local network. *See* paras. 0024-0025 and Figure 3 (*e.g.*, devices 312, 314, and firewall 310). *Schwartz* fails to teach or suggest searching for a firewall at a remote network in the manner described in the claim.

Schwartz also states that "if an address and/or port does not yield a successful connection, then the next time the device will select the most likely address and port 506, it may not include the unsuccessful port." *See* para. 0032. "It is to be understood that select most likely address and port 506 is

based upon a database of addresses and ports and that this database changes." *See* para. 0032. Therefore, *Schwartz* fails to teach or suggest that a request to transmit data includes a primary address of the destination that is used if a firewall is not detected and a secondary address of the destination that is used if a firewall is detected, as described in the claim. Rather, *Schwartz* uses whatever port the non-traditional device discerns is most likely to establish a connection with the local firewall. As such, *Schwartz* fails to teach or suggest that a request to transmit data includes a primary address and a secondary address of a firewall associated with a destination. As previously indicated, *Schwartz* teaches that a local device is configured to operate with a local firewall by attempting different addresses for the local firewall. Accordingly, nowhere does it teach or suggest attempting to communicate with a firewall associated with a destination at a remote network in a manner described by the claim.

For at least these reasons, *Schwartz* fails to anticipate claim 29. In the Office Action of July 24, 2006, it states that "the client shown in Fig. 3 may have to pass the firewall associated with the appliances in the remote network to control them." Page 3. However, nowhere in *Schwartz* does it state that the clients 308-1...308-N shown in Fig. 3 perform the method for firewall traversal disclosed in the reference. Rather, the non-traditional devices 314-1...314-Q are disclosed to employ the method for firewall traversal described in the reference which states "This information must be transferred from the non-traditional device across the LAN 311 through the firewall 310 to a destination." Para. 0025. Another example is provided in *Schwartz* of a home entertainments system 314-5 that must traverse the local firewall 310 to

access the manufacturer's site. As such, *Schwartz* does not teach "means for searching for a firewall at the remote network, the firewall being configured to prohibit communication to the destination by a primary communication protocol and allow communication to the destination via the secondary communication protocol . . . wherein the request comprises at least the following: a primary address and a secondary address of the destination, the primary address being related to the primary communication protocol and the secondary address being related to the secondary communication protocol," as recited in claim 29.

Moreover, the Office Action of July 24, 2006 states that "It is true that Scharwtz won't try the primary address again if it fails, but it clearly tries it the first time, which was before the connection failed. Therefore, the address of the primary and secondary protocols must be received by the device that initiates the connection." Page 4. Applicants respectfully disagree, since *Schwartz* teaches that an address may be obtained by sniffing network traffic and therefore does not have to be "received by the device that initiates the connection." Further, *Schwartz* does not teach or suggest that a request to transmit data comprises both the primary address and secondary address of the destination, as described in claim 29.

For at least these reasons, *Schwartz* fails to anticipate claim 29, and the rejection of claim 29 should be withdrawn.

G. Applicant's Claims 30 and 33-34

Because independent claim 29 is allowable over the cited art of record, dependent claims 30 and 33-34 (which depend from independent claim 29) are allowable as a matter of law for at least the reason that the dependent

claims 30 and 33-34 contain all the features of independent claim 29. For at least this reason, the rejection of claims 30 and 33-34 should be withdrawn.

Additionally and notwithstanding the foregoing reasons for allowability of claims 30 and 33-34, these claims recite further features and/or combinations of features (as is apparent by examination of the claims themselves) that are patentably distinct from the cited art of record. Hence, there are other reasons why these dependent claims are allowable.

Accordingly, the rejections to these claims should be withdrawn.

H. Applicant's Claim 35

As provided in independent claim 35, Applicant claims:

> A data transmission program stored on a computer-readable medium, the transmission program comprising:
> logic configured to facilitate the transmission of data to a remote network by utilizing a secondary communication protocol;
> ***logic configured to search for a firewall at the remote network, wherein the firewall is configured to prohibit communication to a recipient device at the remote network via a primary communication protocol and allow communication via the secondary communication protocol;*** and
> ***logic configured to automatically configure communication for the secondary communication protocol upon detecting the firewall;*** and
> ***logic configured to receive a request to transmit the data to the recipient device, the request comprising of at least the following: a primary address and a secondary address of the recipient device, the primary address being related to the primary communication protocol and the secondary address being related to the secondary communication protocol.***

(Emphasis added).

Applicant respectfully submits that independent claim 35 is allowable for at least the reason that *Schwartz* does not disclose, teach, or suggest at

least "logic configured to search for a firewall at a remote network, wherein the firewall is configured to prohibit communication to a recipient device at the remote network via a primary communication protocol and allow communication via the secondary communication protocol," "logic configured to automatically configure communication for the secondary communication protocol upon detecting the firewall," and "logic configured to receive a request to transmit the data to the recipient device, the request comprising of at least the following: a primary address and a secondary address of the recipient device, the primary address being related to the primary communication protocol and the secondary address being related to the secondary communication protocol," as recited and emphasized above.

Rather, *Schwartz* discloses at most a system for configuring a device to communicate through a firewall on a local network, where the device is also located on the local network. *See* paras. 0024-0025 and Figure 3 (*e.g.*, devices 312, 314, and firewall 310). *Schwartz* fails to teach or suggest searching for a firewall at a remote network in the manner described in the claim.

Schwartz also states that "if an address and/or port does not yield a successful connection, then the next time the device will select the most likely address and port 506, it may not include the unsuccessful port." *See* para. 0032. "It is to be understood that select most likely address and port 506 is based upon a database of addresses and ports and that this database changes." *See* para. 0032. Therefore, *Schwartz* fails to teach or suggest that a request to transmit data includes a primary address of the destination that is used if a firewall is not detected and a secondary address of the destination

that is used if a firewall is detected, as described in the claim. Rather, *Schwartz* uses whatever port the non-traditional device discerns is most likely to establish a connection with the local firewall. As such, *Schwartz* fails to teach or suggest that a request to transmit data includes a primary address and a secondary address of a firewall associated with a destination. As previously indicated, *Schwartz* teaches that a local device is configured to operate with a local firewall by attempting different addresses for the local firewall. Accordingly, nowhere does it teach or suggest attempting to communicate with a firewall associated with a destination at a remote network in a manner described by the claim.

For at least these reasons, *Schwartz* fails to anticipate claim 35. In the Office Action of July 24, 2006, it states that "the client shown in Fig. 3 may have to pass the firewall associated with the appliances in the remote network to control them." Page 3. However, nowhere in *Schwartz* does it state that the clients 308-1...308-N shown in Fig. 3 perform the method for firewall traversal disclosed in the reference. Rather, the non-traditional devices 314-1...314-Q are disclosed to employ the method for firewall traversal described in the reference which states "This information must be transferred from the non-traditional device across the LAN 311 through the firewall 310 to a destination." Para. 0025. Another example is provided in *Schwartz* of a home entertainments system 314-5 that must traverse the local firewall 310 to access the manufacturer's site. As such, *Schwartz* does not teach "logic configured to search for a firewall at a remote network . . . and logic configured to receive a request to transmit the data to the recipient device, the request comprising of at least the following: a primary address and a

secondary address of the recipient device, the primary address being related to the primary communication protocol and the secondary address being related to the secondary communication protocol," as recited in claim 35.

Moreover, the Office Action of July 24, 2006 states that "It is true that Scharwtz won't try the primary address again if it fails, but it clearly tries it the first time, which was before the connection failed. Therefore, the address of the primary and secondary protocols must be received by the device that initiates the connection." Page 4. Applicants respectfully disagree, since *Schwartz* teaches that an address may be obtained by sniffing network traffic and therefore does not have to be "received by the device that initiates the connection." Further, *Schwartz* does not teach or suggest that a request to transmit data comprises both the primary address and secondary address of the destination, as described in claim 35.

For at least these reasons, *Schwartz* fails to anticipate claim 35, and the rejection of claim 35 should be withdrawn.

I. Applicant's Claims 37 and 39-41

Because independent claim 35 is allowable over the cited art of record, dependent claims 37 and 39-41 (which depend from independent claim 35) are allowable as a matter of law for at least the reason that the dependent claims 37 and 39-41 contain all the features of independent claim 35. For at least this reason, the rejection of claims 37 and 39-41 should be withdrawn.

Additionally and notwithstanding the foregoing reasons for allowability of claims 37 and 39-41, these claims recite further features and/or combinations of features (as is apparent by examination of the claims themselves) that are patentably distinct from the cited art of record.

Hence, there are other reasons why these dependent claims are allowable. Accordingly, the rejections to these claims should be withdrawn.

VIII. Conclusion

In summary, it is Applicant's position that Applicant's claims are patentable over the applied cited art references and that the rejection of these claims should be withdrawn. Appellant therefore respectfully requests that the Board of Appeals overturn the Examiner's rejection and allow Applicant's pending claims.

Respectfully submitted,

By: _____

Charles W. Griggers
Registration No. 47,283

Claims Appendix under 37 C.F.R. § 41.37(c)(1)(viii)

The following are the claims that are involved in this Appeal.

1. A method of transmitting data across a firewall, the method comprising:

receiving a request to transmit data to a destination at a remote network;

searching for a firewall associated with the destination at the remote network, the firewall being configured to prohibit communication to the destination via a primary communication protocol and allow communication to the destination via a secondary communication protocol;

if the firewall is detected, automatically configuring the data for communication with the secondary communication protocol; and

transmitting the data to the destination by utilizing the secondary communication protocol, wherein the request to transmit the data to the destination comprises a primary address of the destination related to the primary communication protocol and a secondary address of the destination related to the secondary communication protocol.

2. The method of claim 1, further comprising:

transmitting the data to the destination by utilizing the primary communication protocol if the firewall is not detected.

3. Canceled

4. The method of claim 1, wherein the destination is a printer and a print job comprises the data that is requested to be transmitted.

5. The method of claim 1, wherein searching for the firewall comprises pinging the primary address of the destination.

6. The method of claim 2, wherein searching for the firewall comprises:

scanning the destination to find an open port, the open port being related to the primary communication protocol; and

detecting the firewall, if present, upon not finding the open port.

7. The method of claim 2, wherein searching for the firewall comprises:

attempting to transmit the data via the primary communication protocol, such that a failure to successfully transmit the data via the primary communication protocol would signify the firewall is present.

8. The method of claim 2, wherein the primary communication protocol is any one or combination of the following: the Hyper-Text Transfer Protocol (HTTP), the Transfer Control Protocol (TCP), the Internet Protocol (IP), the File Transfer Protocol (FTP), and the User Datagram Protocol (UDP).

9. The method of claim 1, wherein the secondary communication protocol is an electronic mail (email) protocol and the secondary address is an email address; and further wherein automatically configuring the data for communication comprises:

generating an email;

addressing the email to the secondary address; and

populating the email with pertinent information that correlates to the data.

10. The method of claim 9, wherein automatically configuring the data for communication further comprises: placing the data in the email.

11. The method of claim 9, wherein automatically configuring the data for communication further comprises: attaching the data to the email, the data being stored in a file.

12. The method of claim 9, wherein the information that is populated in the email comprises a reference to a remote location where the data is stored and is accessible from the destination.

13. The method of claim 1, wherein the secondary communication protocol is the File Transfer Protocol (FTP) and the secondary address is an FTP address.

14. A system for rerouting the transmission of data to avoid a firewall, the system comprising:

a transmission device configured to search for a firewall protecting a destination at a remote network, the firewall at the remote network being configured to prohibit communication to the destination via a primary communication protocol and allow communication to the destination via a secondary communication protocol, the transmission device is further configured to, upon detection of the firewall, automatically configure the data for communication over the secondary communication protocol and transmit the data by utilizing the secondary communication protocol, wherein the transmission device is further configured to receive a request to transmit the data to the destination and the request comprises at least the following:

a primary address and a secondary address of the destination, the primary address being related to the primary communication protocol and the secondary address being related to the secondary communication protocol and wherein the transmission device is further configured to, upon not detecting the firewall, transmit the data to the destination by utilizing the primary communication protocol.

15-16. Canceled

17. The system of claim 14, wherein the transmission device is further configured to search for the firewall by scanning the destination to find an open port, the open port being related to the primary communication protocol, upon not finding the open port, the firewall is detected.

18. The system of claim 14, wherein the transmission device is further configured to search for the firewall by pinging the primary address of the destination.

19. The system of claim 14, wherein the transmission device is further configured to search for the firewall by attempting to transmit the data via the primary communication protocol, such that a failure to successfully transmit the data via the primary communication protocol would signify the firewall is present.

20. The system of claim 14, wherein the secondary communication protocol is an electronic mail (email) protocol.

21. The system of claim 20, wherein the secondary address is an email address and wherein the transmission device is further configured to automatically configure communication by: generating an email;

addressing the email to the secondary address; and

populating the email with pertinent information that correlates to the data.

22. The system of claim 21, wherein the transmission device is further configured to automatically configure the data for communication by placing the data in the email.

23. The system of claim 21, wherein the transmission device is further configured to automatically configure the data for communication by attaching the data to the email, the data being stored in a file.

24. The system of claim 21, wherein the information that is populated in the email comprises a reference to a remote location where the data is stored and is accessible from the destination.

25. The system of claim 14, wherein the secondary communication protocol is the File Transfer Protocol (FTP) and wherein the secondary address is an FTP address.

26. The system of claim 14, wherein the primary communication protocol is any one or combination of the following: the Hyper-Text Transfer Protocol (HTTP), the Transfer Control Protocol (TCP), the Internet Protocol (IP), the File Transfer Protocol (FTP), and the User Datagram Protocol (UDP).

27. The system of claim 14, further comprising: a recipient device configured to be the destination, the recipient device further configured to communicate with the primary and secondary communication protocol.

28. The system of claim 27, wherein the recipient device is a printer and a print job comprises the data.

29. A transmission device configured to transmit data to a destination, the transmission device comprising:

means for transmitting the data to the destination at a remote network by utilizing a secondary communication protocol;

means for searching for a firewall at the remote network, the firewall being configured to prohibit communication to the destination by a primary communication protocol and allow communication to the destination via the secondary communication protocol;

means for automatically configuring the data for communication for the secondary communication protocol upon detecting the firewall; and

means for receiving a request to transmit the data to the destination, wherein the request comprises at least the following:

a primary address and a secondary address of the destination, the primary address being related to the primary communication protocol and the secondary address being related to the secondary communication protocol.

30. The device of claim 29, further comprising means for transmitting the data by utilizing the primary communication protocol, wherein upon not detecting the firewall, the data is transmitted by utilizing the primary communication protocol.

31-32. Canceled

33. The device of claim 30, wherein the secondary communication protocol is an electronic mail (email) protocol.

34. The device of claim 30, wherein the secondary address is an email address and wherein the means for automatically configuring the data for communication for the secondary communication protocol comprises:

means for generating an email;

means for addressing the email to the secondary address;

means for populating the email with pertinent information that correlates to the data; and

means for populating the email with the data.

35. A data transmission program stored on a computer-readable medium, the transmission program comprising:

logic configured to facilitate the transmission of data to a remote network by utilizing a secondary communication protocol;

logic configured to search for a firewall at the remote network, wherein the firewall is configured to prohibit communication to a recipient device at the remote network via a primary communication protocol and allow communication via the secondary communication protocol; and

logic configured to automatically configure communication for the secondary communication protocol upon detecting the firewall; and

logic configured to receive a request to transmit the data to the recipient device, the request comprising of at least the following: a primary address and a secondary address of the recipient device, the primary address being related to the primary communication protocol and the secondary address being related to the secondary communication protocol.

36. Canceled

37. The program of claim 35, further comprising logic configured to facilitate the transmission of the data by utilizing the primary communication protocol, wherein upon not detecting the firewall, the data is transmitted by utilizing the primary communication protocol.

38. Canceled

39. The program of claim 35, wherein the secondary address is an electronic mail (email) address and the secondary communication protocol is an email protocol; and wherein the logic configured to automatically configure the data for communication for the secondary communication protocol comprises:

logic configured to generate an email;

logic configured to address the email to the secondary address;

logic configured to populate the email with pertinent information that correlates to the data; and

logic configured to populate the email with the data.

40. The program of claim 35, wherein the secondary communication protocol is the File Transfer Protocol (FTP) and the secondary address is an FTP address.

41. The program of claim 35, wherein the primary communication protocol is any one or combination of the following: the Hyper-Text Transfer Protocol (HTTP), the Transfer Control Protocol (TCP), the Internet Protocol (IP), the File Transfer Protocol (FTP), and the User Datagram Protocol (UDP).

Evidence Appendix under 37 C.F.R. § 41.37(c)(1)(ix)

There is no extrinsic evidence to be considered in this Appeal. Therefore, no evidence is presented in this Appendix.

Related Proceedings Appendix under 37 C.F.R. § 41.37(c)(1)(x)

There are no related proceedings to be considered in this Appeal. Therefore, no such proceedings are identified in this Appendix.